UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF OKLAHOMA

MARIA RUSKIEWICZ, on behalf of herself, and all others similarly situated,	)	
Plaintiff	)	
v.	)	Civil Action No. CIV-23-303-D
OKLAHOMA CITY UNIVERSITY;	)	
Defendant.	)	

CLASS ACTION COMPLAINT

Plaintiff, Maria Ruskiewicz ("Plaintiff" or "Ruskiewicz") individually and on behalf of all others similarly situated, complains and alleges as follows against Defendant, Oklahoma City University ("Defendant" or "OCU") based on personal knowledge, on the investigation of her counsel, and on information and belief as to all other matters:

INTRODUCTION

1. This is a civil action seeking monetary damages and injunctive and declaratory relief from Defendant OCU, arising from its failure to safeguard certain Personally Identifying Information[1] ("PII") and other sensitive, non-public financial information (collectively, "Personal Information") of thousands of its current and former students and employees, as well as others whose personal information was stored on the university's systems.

2. OCU's failure to safeguard these individuals' PII resulted in Defendant's email

[1] The Federal Trade Commission defines "personally identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8). To be clear, according to Defendant, not every type of information included in that definition was compromised in the breach.

systems being unauthorizedly accessed by hackers and the Personal Information of students, employees, and others therein, including of Plaintiff and the proposed Class Members, being disclosed, stolen, compromised, and misused, causing widespread and continuing injury and damages.

3. On information and belief, on or around July 23, 2022, OCU's network was unauthorizedly infiltrated and encrypted, resulting in the unauthorized disclosure of the Personal Information of Plaintiff and the Class Members, including names, addresses, Social Security Numbers, Driver's License/State ID numbers, and passport numbers (the "Data Breach"). *See* OCU Notice of Data Breach to Plaintiff, March 20, 2023 ("Notice Letter" or "Notice"), attached as **Exhibit 1**; and, OCU sample Notice of Data Breach to Maine Attorney General, available at https://apps.web.maine.gov/online/aeviewer/ME/40/752a741d-e111-4454-afae-e0cef5913242.shtml (last accessed April 1, 2023).

4. On information and belief, approximately 27,229 persons were impacted by the Data Breach.[2]

5. As explained below, Plaintiff and Members of the Class have suffered significant injury and damages due to the Data Breach permitted to occur by OCU, and the resulting monetary damages including out-of-pocket expenses, including those associated with the reasonable mitigation measures they were forced to employ, and other damages. Plaintiff and the Class also now forever face an amplified risk of *further* misuse, fraud, and identity theft due to their sensitive Personal Information falling into the hands of cybercriminals as a result of the tortious conduct of Defendant.

[2] OCU report to Maine Attorney General, available at: https://apps.web.maine.gov/online/aeviewer/ME/40/752a741d-e111-4454-afae-e0cef5913242.shtml (last accessed April 1, 2023).

6. As a consequence of the Data Breach, Plaintiff and the Proposed Class Members' sensitive Personal Information have been released into the public domain and they have had to, and will continue to have to, spend time, effort, and money to protect themselves from fraud and identity theft.

7. Further, and to compound the harm, Defendant waited over eight (8) months before Defendant publicly disclosed the incident. While the Notice Letter states that Defendant detected the Data Breach by July 23, 2022, Defendant did not publish the Notice Letter until March 20, 2023. *Id.*

8. As a result of the Data Breach, Plaintiff and the Proposed Class Members have been required to take measures to deter and detect identity theft and fraud. Plaintiff and the Proposed Class Members have been required to take the time and effort, which they otherwise would have dedicated to other life demands, to mitigate the actual and potential impact of the Data Breach including, among other things, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring their credit reports, financial accounts, explanations of benefits, and medical accounts for unauthorized activity.

9. Defendant disregarded the rights of Plaintiff and the Proposed Class Members by failing to take and implement adequate and reasonable measures to ensure that the Personal Information it stores was safeguarded; failing to take available steps to prevent the Data Breach from happening; failing to follow the mandatory, applicable, and appropriate protocols, policies, and procedures; and failing to timely notify Plaintiff and the Proposed Class Members.

10. As the direct result of Defendant's actions, the Personal Information of Plaintiff and the Proposed Class Members was compromised and stolen by unauthorized third parties.

11. Because this same information remains stored in Defendant's systems, Plaintiff and the Proposed Class members have an interest in ensuring that Defendant takes the appropriate measures to protect their information against future unauthorized disclosures.

12. On behalf of herself and the Class preliminarily defined below, Plaintiff brings causes of action for negligence, negligence *per se*, breach of express and implied contractual duties, unjust enrichment, invasion of privacy, and violation of the Oklahoma Consumer Protection Act. Plaintiff seeks damages and injunctive and declaratory relief arising from OCU's failure to adequately protect her highly sensitive Personal Information.

PARTIES

13. Plaintiff, Maria Ruskiewicz, is a natural person who resides in Marinette County, Wisconsin. Plaintiff is among thousands of individuals whose Personal Information was disclosed to unauthorized third parties during the Data Breach.

14. Plaintiff is a former student and graduate of OCU School of Law.

15. Plaintiff paid tuition and fees for educational services provided by the Defendant to the Plaintiff.

16. Plaintiff received a notice from OCU stating that her Personal Information including her name, address, Social Security Number, Driver's License/State ID number, and passport number were potentially compromised during the Data Breach.

17. Defendant, Oklahoma City University is a private university located in Oklahoma City, Oklahoma.

JURISDICTION AND VENUE

18. Jurisdiction is proper in this Court pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), because: (i) there are more than one hundred (100) Class Members; (ii) the

aggregate amount in controversy exceeds five million dollars ($5,000,000.00), exclusive of interest and costs; and (iii) some Class Members are citizens of states different than OCU.

19. This Court has personal jurisdiction over OCU because it regularly and systematically transacts business in the State of Oklahoma, such that it can reasonably anticipate defending a lawsuit here.

20. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to these claims occurred in this district, and/or or a substantial part of property that is the subject of this action is situated herein.

FACTUAL ALLEGATIONS

A. Plaintiff and the Class Members entrusted their Personal Information to OCU

21. Defendant, OCU, is a private, liberal arts and sciences university in Oklahoma City, Oklahoma.

22. In the ordinary course of providing educational services, students are required to provide Defendant with sensitive, personal, and private information such as name, address, phone number and email address; date of birth; demographic information; social security number; photo identification; employer information; and other information that may be deemed necessary by the Defendant. Similarly, OCU employees are required to provide OCU with Personal Information as a condition of employment.

23. OCU acquired, collected, and stored a massive amount of said Personal Information of its students, employees, and others, including Ruskiewicz and the Members of the proposed Class, which it stored in its electronic systems.

24. By obtaining, collecting, using, and deriving a benefit from its students' and employees' Personal Information, OCU assumed legal and equitable duties to those individuals

and knew or should have known that it was responsible for protecting their Personal Information from unauthorized disclosure.

25. Plaintiff has taken reasonable steps to maintain the confidentiality of her Personal Information. Plaintiff, as a former student, relied on OCU to keep her Personal Information confidential and securely maintained, to use this information for authorized purposes and disclosures only.

26. In addition, OCU maintains a Confidentiality and Privacy Policy ("Privacy Policy")[3] on its website, where it acknowledges its obligations to safeguard Personal Information under the family Educational Rights and Privacy Act of 1974, (FERPA), the Health Information Portability and Accountability Act (HIPAA); and the Gramm-Leach-Bliley Act (GLBA):

> **Oklahoma City University makes every effort to abide by all applicable Federal and State regulations, guidelines, statutes and procedures pertaining to confidentiality and privacy, specifically:**
>
> - **The family Educational Rights and Privacy Act of 1974, as Amended (FERPA);**
> - **The Health Information Portability and Accountability Act (HIPAA); and**
> - **The Gramm-Leach-Bliley Act (GLB)**
>
> **FERPA protects the privacy of student education records. HIPAA controls the release of Protected Health Information (PHI) dealing primarily with patient information. GLB safeguards customer financial information.**

(Exhibit 2).

27. OCU further acknowledges in its Privacy Policy that the kind of Personal

---

[3] *See* **Exhibit 2**, https://cdn2.assets-servd.host/oklahomacity-university/production/human-resources/docs/Confidentiality-and-privacy.pdf (last accessed April 1, 2023).

Information described in the Notice Letter are confidential and must remain secure from public disclosure:

> **As an employee of Oklahoma City University, you may have access to student, employee or other person's academic, personal, health and financial records that may contain individually identifiable information. This information is considered confidential. Examples of private, confidential information include, but are not limited to: student academic information (grades, courses taken, schedules, test scores, advising records), educational services received, social security number, gender, ethnicity, citizenship, veteran and disability status, health records, financial information, financial aid applications, copies of tax returns and passwords.**
>
> **It is important to handle all confidential information with discretion and it should only be disclosed to others who have a need to know for legitimate business reasons. In most cases, data of an individually identifiable nature shall remain secure from public disclosure (release to third parties) without specific permission from the individual to whom the data applies, unless law allows disclosure without consent. Improper disclosure of this information to any unauthorized person is prohibited under Federal law and could subject you to criminal and civil penalties imposed by law. Any such willful or unauthorized disclosure also violates university policy and it will be cause for disciplinary action, up to and including termination from employment regardless of whether criminal or civil penalties are imposed.**
>
> **Student and administrative data originated or stored in university computer systems is university property. Only data that is required for one's job should be accessed. To safeguard computer data, employees should not share computer login information or leave their computer signed on when away from their desk for extended periods. Computer passwords should be changed regularly. Employees should refer to the University Computer and Network Use Policy for further guidance.**
>
> **Employees should handle all confidential information with discretion, safeguarding it when in use, filing it in locked file cabinets when not in use, disposing of it properly (i.e. shredding) when no longer needed and not disclosing or discussing it with any unauthorized person while working for Oklahoma City University, or after employment at the University.**

Id.

28. Notably, the Privacy Policy gives no warning or mention to its employees about how to protect confidential information from unauthorized cyberattacks such as phishing scams.

29. The Data Breach that is the subject of this civil action is not contemplated or permitted by OCU's website Privacy Policy.

30. Plaintiff and the proposed Class Members entrusted their Personal Information to OCU with the expectation and implied mutual understanding that OCU would strictly maintain the confidentiality of the information and undertake adequate measures to safeguard it from theft or misuse.

31. Plaintiff and the proposed Class Members would not have entrusted OCU with their highly sensitive Personal Information if they had known that OCU would fail to take adequate measures to protect it from unauthorized use or disclosure.

B. Plaintiff's and the Class Members' Personal Information was Unauthorizedly Disclosed and Compromised in the Data Breach

32. Plaintiff Ruskiewicz was a student at OCU from 2009 to 2011.

33. As a prerequisite to enrollment, Plaintiff and the Class Members disclosed their non-public and sensitive Personal Information to OCU, with the implicit understanding that their Personal Information would be kept confidential. This understanding was based on all the facts and circumstances attendant to their enrollment there, and the express, specific, written representations made by OCU and its agents.

34. Plaintiff and the Class Members reasonably relied upon OCU's representations to her detriment and would not have provided their sensitive Personal Information to OCU if not for OCU's explicit and implicit promises to adequately safeguard that information.

35. On or about March 20, 2023, OCU began sending Notice Letters to the Class Members notifying them that their Personal Information had been compromised during the Data Breach. Ruskiewicz received the Notice on or around March 27, 2023. *See* **Exhibit 1.**

36. According to OCU's Notice Letter, on July 23, 2022, Defendant "detected and

stopped a network security incident" wherein an "unauthorized third party infiltrated [its] network and encrypted some of [its] data." *Id.* Defendant stated it "immediately shut off access to the impacted systems and engaged specialized third-party forensic and technical resources to respond to the incident." *Id.*

37. OCU further indicated that through its investigation, it learned "that the unauthorized party obtained some personal identifiable information of current and prior students and others with information held on the university's systems." *Id.* The Notice Letter addressed to Plaintiff indicated the "following categories of your information may have been exposed to the unauthorized party during the compromise: Name, Address, Social Security Number, Driver's License/State ID Number, and Passport Number." *Id.*

38. OCU urged those affected by the Data Breach to "monitor your credit reports for suspicious or unauthorized activity . . . contact your financial institutions and all credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file." *Id.*

39. In addition, OCU's Notice provided a toll-free telephone number for affected persons receiving the Notice to call IDX for their questions to be addressed. *Id.*

40. Despite OCU claiming in its Notice that it had no reason to believe any impacted information had been misused, it offered complimentary credit monitoring and identity protection services through IDX.

41. As a result of this Data Breach, the Personal Information of Plaintiff and the proposed Class Members, believed to be approximately 27,229 individuals, was unauthorizedly disclosed and compromised in the Data Breach.

42. The Data Breach was preventable and a direct result of OCU's failure to implement

adequate and reasonable cyber-security procedures and protocols necessary to protect individuals' Personal Information.

43. In addition, while OCU alleges it discovered the Data Breach on January 27, 2023, as reported to the Maine Attorney General, OCU's own Notice Letter indicates that it discovered the breach immediately, on July 23, 2022, and that an investigation was instituted, but it failed to notify affected persons in a timely manner until March 20, 2023.[4]

C. OCU Failed to Sufficiently Protect the Personal Information that Plaintiff and the Proposed Class Members Had Entrusted to It.

44. Over the past several years, data breaches have become alarmingly commonplace. In 2016, the number of data breaches in the U.S. exceeded 1,000, a 40% increase from 2015.[5] The next year, that number increased by nearly 50%.[6]

45. The Personal Information stolen in the Data Breach is significantly more valuable than the loss of, say, credit card information in a large retailer data breach. Victims affected by those retailer breaches could avoid much of the potential future harm by simply cancelling credit or debit cards and obtaining replacements. The information stolen in the Data Breach— most notably names and Social Security Numbers —is difficult, if not impossible, to change.

46. This kind of data, as one would expect, demands a much higher price on the dark web. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit

---

[4] OCU report to Maine Attorney General, available at: https://apps.web.maine.gov/online/aeviewer/ME/40/752a741d-e111-4454-afae-e0cef5913242.shtml (last accessed March 31, 2023).

[5] *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout*, IDENTITY THEFT RESOURCE CENTER ("ITRC") (Jan. 19, 2017), https://www.idtheftcenter.org/data-breaches-increase-40-percent-in-2016-finds-new-report-from-identity-theft-resource-center-and-cyberscout/.

[6] *2017 Annual Data Breach Year-End Review*, ITRC, (Jan. 25, 2018), https://www.idtheftcenter.org/images/breach/2017Breaches/2017AnnualDataBreachYearEndReview.pdf.

card information, personally identifiable information… [is] worth more than 10x on the black market."[7]

47. PII data for sale is so valuable because PII is so broad, and it can therefore be used for a wide variety of criminal activity such as creating fake IDs, buying medical equipment and drugs that can be resold on the street, or combining PII with false provider numbers to file fake claims with insurers.

48. The value of Plaintiff's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

49. Email phishing schemes "remain[] the primary attack vector for nine out of 10 cyberattacks."[8] OCU did not elaborate on how the Data Breach happened, other than that an unauthorized third party infiltrated its network.

50. Companies can mount two primary defenses to phishing scams: employee education and technical security barriers.

51. Employee education is the process of adequately making employees aware of common phishing attacks and implementing company-wide policies requiring the request or transfer of sensitive personal or financial information only through secure sources to known recipients. Employee education and secure file-transfer protocols provide the easiest method to

---

[7] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT WORLD (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hackpersonal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

[8] Benishti, Eyal, *How to Safeguard Hospital Data from Email Spoofing Attacks*, INSIDE DIGITAL HEALTH, (Apr. 4, 2019), https://www.idigitalhealth.com/news/how-to-safeguard-hospital-data-from-email-spoofing-attacks.

assist employees in properly identifying fraudulent e-mails and preventing unauthorized access to PII.

52. From a technical perspective, companies can also greatly reduce the flow of phishing e-mails by implementing certain security measures governing e-mail transmissions. Companies can use a simple email validation system that allows domain owners to publish a list of IP addresses that are authorized to send emails on their behalf to reduce the amount of spam and fraud by making it much harder for malicious senders to disguise their identities. Companies can also use email authentication that blocks email streams that have not been properly authenticated.

i. OCU failed to adhere to FTC guidelines

53. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making.[9] To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as OCU, should employ to protect against the unlawful exposure of Personal Information.

54. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[10] The guidelines explain that businesses should:

a. protect the personal information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

[9] *Start with Security: A Guide for Business*, FED. TRADE COMM'N (Sep. 2, 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.
[10] *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N (Sep. 28, 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

e. implement policies to correct security problems.

The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

55. The FTC recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[11]

56. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect PII, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

57. OCU's failure to employ reasonable and appropriate measures to protect against unauthorized access to PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

58. OCU failed to adequately train its employees on even the most basic of cybersecurity protocols, including:

a. How to detect phishing emails and other scams including providing employees examples of these scams and guidance on how to verify if emails are legitimate;

[11] *See Start with Security*, *supra* n.40.

b. Effective password management and encryption protocols for internal and external emails;

c. Avoidance of responding to emails that are suspicious or from unknown sources;

d. Locking, encrypting and limiting access to computers and files containing sensitive information; and

e. Implementing guidelines for maintaining and communicating sensitive data.

59. OCU's failure to implement these rudimentary measures made it an easy target for the Data Breach that came to pass.

ii. OCU failed to adhere to GLBA guidelines

60. The Federal Trade Commission considers Title IV-eligible institutions, like OCU, that participate in Title IV Educational Assistance Programs as "financial institutions" and subject to the Gramm-Leach-Bliley Act (16 CFR 313.3(k)(2)(vi) ("GLBA").

61. Defendant expressly acknowledges in its Privacy Policy that it has a duty to remain in compliance with the mandates under GLBA to protect the privacy, security, and confidentiality of personally identifiable financial records and information of its students.

62. The GLBA's Safeguard Rule requires the following in relevant parts:

> **§ 314.3 Standards for safeguarding customer information.**
>
> (a) *Information security program.* You shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue. Such safeguards shall include the elements set forth in § 314.4 and shall be reasonably designed to achieve the objectives of this part, as set forth in paragraph (b) of this section.

(b) *Objectives.* The objectives of section 501(b) of the Act, and of this part, are to:

(1) Insure the security and confidentiality of customer information;

(2) Protect against any anticipated threats or hazards to the security or integrity of such information; and

(3) Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

§ 314.4 Elements.

In order to develop, implement, and maintain your information security program, you shall:

. . . (b) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including:

(1) Employee training and management;

(2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and

(3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.

(c) Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

. . . (e) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program.

63. The GLBA, which Defendant expressly acknowledges in its Privacy Policy, creates a duty for Defendant to safeguard Plaintiff's and the Class Members' Personal Information.

64. Defendant was obligated by federal law, its own policies, and industry standards to

keep Plaintiff's and Class Members' Personal Information entrusted to Defendant confidential and to protect it from unauthorized access and disclosure.

65. However, Defendant has failed to adequately implement such policies. This failure to implement has resulted in the Data Breach at issue.

66. Defendant's policies and procedures to safeguard the Personal Information of the Plaintiff and other Proposed Class Members were inadequate, insufficient, and non-compliant with its statutory obligations.

67. Plaintiff and Proposed Class Members provided their Personal Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

68. Plaintiff and Proposed Class Members reasonably believed that Defendant would maintain their Personal Information in a secure manner and relied upon this understanding when providing said information to the Defendant.

69. Had Plaintiff and Proposed Class Members known that Defendant would not maintain their information in a reasonably secure manner, they would not have provided their Personal Information to Defendant.

70. Defendant could have easily prevented this Data Breach. Defendant is aware of the value of Personal Information and the risks associated with unauthorized disclosure of this information, yet Defendant failed to implement adequate measures to protect its students, employees, and other affiliated individuals' Personal Information.

71. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard the Personal

Information maintained on its systems. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to implement its promised Privacy Policy;

c. Failing to adhere to FTC and GLBA standards;

d. Failing to adequately protect Proposed Class Members' Personal Information;

e. Failing to properly monitor its own data security systems for existing intrusions; and

f. Failing to provide timely notice of the breach.

D. Plaintiff and the Class Members were Significantly Injured by the Data Breach

72. As a result of OCU's failure to prevent the Data Breach, Plaintiff Ruskiewicz and the Class Members have suffered and will continue to suffer significant injury and damages. They have suffered or are at increased risk of suffering:

a. Misuse of Personal Information;

b. The loss of the opportunity to control how Plaintiff's and the Class Members' Personal Information is used;

c. The diminution in value of their Personal Information;

d. The compromise, publication and/or theft of their Personal Information;

e. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud, including the purchase of identity theft protection insurance and detection services;

f. Increased receipt of spams, calls and texts;

g. Lost opportunity costs and lost wages associated with the time and effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;

h. Delay in receipt of tax refund monies;

i. Unauthorized use of stolen Personal Information;

j. The continued risk to their Personal Information, which remains in the possession of OCU and is subject to further breaches so long as it fails to undertake appropriate measures to protect the Personal Information in their possession; and

k. Current and future costs related to the time, effort, and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

73. As a result of the Data Breach, Plaintiff and the Class Members now face, and will continue to face, a heightened risk of identity theft and fraud for the rest of their lives.

74. As a long-standing member of the higher educational community, OCU knew or should have known the importance of safeguarding Personal Information entrusted to it and of the foreseeable consequences of a breach. Despite this knowledge, however, OCU failed to undertake adequate cyber-security measures to prevent the Data Breach email attack from happening.

75. Although OCU has offered affected victims complimentary credit monitoring and identity protection services through IDX, this will not adequately compensate Ruskiewicz and the Class Members for the injuries and damages resulting from the Data Breach which Defendant

failed to prevent.

76. On the contrary, after conducting a study, the U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[12]

CLASS ACTION ALLEGATIONS

77. Plaintiff brings this action on behalf of herself and all others similarly situated pursuant to Fed. R. Civ. Proc. 23. The Class is preliminarily defined as:

> All individuals whose Personal Information was compromised as a result of the Data Breach with OCU which was announced on or about March 20, 2023.

78. Excluded from the Class are OCU and its subsidiaries and affiliates, officers, directors, and members of their immediate families, and any entity in which it has a controlling interest, the legal representatives, heirs, successors or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

79. Plaintiff reserves the right to modify or amend the definition of the proposed Class and/or to add a subclass(es) if necessary, before this Court determines whether certification is appropriate.

80. *Fed. R. Civ. Proc. 23(a)(1) Numerosity:* The Class is so numerous such that joinder of all Members is impracticable. Upon information and belief, and subject to class discovery, the Class consists of 27,229 current and former students, employees, and other individuals affiliated with OCU, the identity of whom are within the exclusive knowledge of and can be ascertained only by resort to OCU's records. OCU has the administrative capability through its computer

[12] *Victims of Identity Theft, 2012*, U.S. DEP'T OF JUSTICE 10, 11 (Jan. 27, 2014), https://www.bjs.gov/content/pub/pdf/vit12.pdf.

systems and other records to identify all Members of the Class, and such specific information is not otherwise available to Plaintiff.

81. *Fed. R. Civ. Proc. 23(a)(2) Commonality and Fed. R. Civ. Proc. 23(b)(3) Predominance:* There are numerous questions of law and fact common to the Class. As such, there is a well-defined community of interest among the Members of the Class. These questions predominate over questions that may affect only individual Members of the Class because OCU has acted on grounds generally applicable to the Class. Such common legal or factual questions include, but are not limited to:

a. Whether OCU had a duty to protect student, employee, and other OCU-affiliated individuals' Personal Information;

b. Whether OCU knew or should have known of the susceptibility of its systems to a data breach;

c. Whether OCU's security measures to protect its systems were reasonable considering best practices recommended by data security experts;

d. Whether OCU was negligent in failing to implement reasonable and adequate security procedures and practices;

e. Whether OCU's failure to implement adequate data security measures allowed the Data Breach to occur;

f. Whether OCU's conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach, resulting in the unlawful exposure of the Plaintiff's and Class Members' Personal Information;

g. Whether Plaintiff and Class Members were injured and suffered damages or other losses because of OCU's failure to reasonably protect its systems

and data network;

h. Whether Plaintiff and Class Members are entitled to relief;

i. Whether OCU failed to adequately notify Class Members of the compromise of their Personal Information;

j. Whether OCU assumed a fiduciary duty and/or confidential relationship to Class Members when they entrusted it with their Personal Information;

k. Whether OCU breached its contracts with Class Members by failing to properly safeguard their Personal Information and by failing to notify them of the Data Breach;

l. Whether OCU's violation of FTC and GLBA regulations constitutes evidence of negligence or negligence *per se*; and

m. Whether OCU impliedly warranted to Class Members that the information technology systems were fit for the purpose intended, namely the safe and secure processing of Personal Information, and whether such warranty was breached.

82. *Fed. R. Civ. Proc. 23(a)(3) Typicality:* Plaintiff's claims are typical of the claims of all Class Members, because all such claims arise from the same set of facts regarding OCU's failures:

a. to protect Plaintiff's and Class Members' Personal Information;

b. to discover and remediate the security breach of its computer systems more quickly; and

c. to disclose to Plaintiff and Class Members in a complete and timely manner information concerning the security breach and the theft of their Personal

Information.

83. *Fed. R. Civ. Proc. 23(a)(4) Adequacy:* Plaintiff will fairly and adequately protect the interests of the Class. Plaintiff is a more than adequate representative of the Class in that Plaintiff is a victim of the Data Breach, has suffered injury and damages such as misuse and fraudulent activity as a result of the Data Breach, and brings the same claims on behalf of herself and the putative Class. Plaintiff has no interests antagonistic to that of the Class Members. Plaintiff has retained counsel who are competent and experienced in litigating class actions, including class actions following data breaches and unauthorized data disclosures. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

84. *Fed. R. Civ. Proc. 23(b)(2) Injunctive and Declaratory Relief:* OCU has acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Class as a whole.

85. *Fed. R. Civ. Proc. 23(b)(3) Superiority:* It is impracticable to bring Class Members' individual claims before the Court. Class treatment permits many similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently and without the unnecessary duplication of evidence, effort, expense, or the possibility of inconsistent or contradictory judgments that numerous individual actions would engender. The benefits of the class mechanism, including providing injured persons or entities with a method for obtaining redress on claims that might not be practicable to pursue individually, substantially outweigh any difficulties that may arise in the management of this class action.

86. A class action is superior to the other available methods for the fair and efficient adjudication of this controversy because:

a. The unnamed Members of the Class are unlikely to have an interest in

individually controlling the prosecution of separate actions;

b. Concentrating the litigation of the claims in one forum is desirable;

c. Plaintiff anticipates no difficulty in the management of this litigation as a class action; and

d. Plaintiff's legal counsel has the financial and legal resources to meet the substantial costs and legal issues associated with this type of litigation.

87. Plaintiff knows of no unique difficulty to be encountered in the prosecution of this action that would preclude its maintenance as a class action.

88. *Fed. R. Civ. Proc. 23(c)(4) Issue Certification:* Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such issues include, but are not limited to:

a. Whether OCU owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing and safeguarding their Personal Information;

b. Whether OCU's security measures to protect its data systems were reasonable considering best practices recommended by data security experts;

c. Whether OCU's failure to institute adequate protective security measures amounted to negligence;

d. Whether OCU failed to take commercially reasonable steps to safeguard student and employee Personal Information; and

e. Whether adherence to FTC and GLBA data security recommendations, and industry standards on data security would have reasonably prevented the

Data Breach.

89. Finally, all Members of the proposed Class are readily ascertainable. OCU has access to student, employee and applicant names and addresses affected by the Data Breach. Using this information, Class Members can be identified and ascertained for the purpose of providing constitutionally sufficient notice.

COUNT I
NEGLIGENCE

90. Plaintiff Ruskiewicz and the Members of the Class incorporate the above allegations as if fully set forth herein.

91. Defendant OCU owed a duty to Plaintiff and the Members of the Class to exercise reasonable care to safeguard their Personal Information in its possession, based on the foreseeable risk of a data breach and the resulting exposure of their information, as well as on account of the special relationship between Defendant and its students and employees, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

92. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and Members of the Class's Personal Information by disclosing and providing access to this information to third parties and by failing to properly supervise both the manner in which the information was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

93. Further, Defendant owed to Plaintiff and Members of the Class a duty to notify them within a reasonable time frame of any breach to the security of their Personal Information.

Defendant also owed a duty to timely and accurately disclose to Plaintiff and Members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and Members of the Class to take appropriate measures to protect their Personal Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps in an effort to mitigate the harm caused by the Data Breach.

94. OCU owed these duties to Plaintiff and Members of the Class because they are Members of a well-defined, foreseeable, and probable class of individuals who Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff's and Members of the Class's personal information and PII for educational and employment purposes.

95. Plaintiff and Members of the Class were required to provide their Personal Information to Defendant as a condition of applying for educational purposes or employment and/or as a condition of employment, and Defendant retained that information.

96. The risk that unauthorized persons would attempt to gain access to the Personal Information and misuse it was foreseeable. Given that Defendant holds vast amounts of this information, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the Personal Information, whether by email hacking attack, or otherwise.

97. Personal Information is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the Personal Information of Plaintiff and Members of the Class, and the importance of exercising reasonable care in handling it.

98. Defendant OCU breached its duties by failing to exercise reasonable care in supervising its employees and agents, and in handling and securing the Personal Information and

PII of Plaintiff and Members of the Class which actually and proximately caused the Data Breach and Plaintiff's and Members of the Class's injury. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and Members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff's and Members of the Class's injuries-in-fact.

99. As a direct, proximate, and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and Members of the Class have suffered or will suffer injury and damages, including misuse and fraudulent activity, monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

100. Defendant's breach of its common law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff's and Members of the Class's actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT II
NEGLIGENCE *PER SE*

101. Plaintiff and the Class Members incorporate the above allegations as if fully set forth herein.

102. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and the Class Members' Personal Information, PII.

103. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customers' or, in this case, students' and employees' and prospective employees' PII.

104. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff's and the Class Members' sensitive PII.

105. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect its students' and employees' and prospective employees' PII and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII Defendant had required and solicited, collected, and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to students and employees in the event of a breach, which ultimately came to pass.

106. The harm that has occurred in the Data Breach is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class Members.

107. Defendant had a duty to Plaintiff and the Class Members to implement and maintain reasonable security procedures and practices to safeguard their PII.

108. Defendant breached its respective duties to Plaintiff and Members of the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and the Class Members' PII.

109. Defendant's violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

110. But for OCU's wrongful and negligent breach of its duties owed to Plaintiff and the Class, Plaintiff and the Members of the Class would not have been injured.

111. The injury and harm suffered by Plaintiff and the Class Members were the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiff and Members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

112. Had Plaintiff and Members of the Class known that Defendant did not adequately protect students' employees' and prospective employees' PII, Plaintiff and Members of the Class would not have entrusted Defendant with their PII.

113. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class Members have suffered harm, injury, and damages as set forth in the preceding paragraphs.

COUNT III
BREACH OF EXPRESS/IMPLIED CONTRACTUAL DUTY

114. Plaintiff and Members of the Class incorporate the above allegations as if fully set forth herein.

115. Defendant offered to provide education or employment to Plaintiff and Members of the Class in exchange for payment.

116. OCU also required Plaintiff and the Members of the Class to provide Defendant with their Personal Information as a condition of applying for educational or employment positions, and for employees as a condition of receiving renumeration for labor rendered.

117. In turn, and through its Privacy Policy, Defendant agreed it would not disclose

Personal Information it collects to unauthorized persons. Defendant also promised to maintain safeguards to protect their Personal Information.

118. Plaintiff and the Members of the Class accepted Defendant's offer by providing Personal Information to OCU, in applying for education or employment, and providing labor to Defendant and receiving renumeration.

119. The agreement was supported by adequate consideration, as it was an exchange of labor for money.

120. Implicit in the Parties' agreement was that Defendant would provide Plaintiff and Members of the Class with prompt and adequate notice of any and all unauthorized access and/or theft of their Personal Information.

121. Plaintiff and the Members of the Class would not have entrusted their Personal Information to Defendant in the absence of such agreement with Defendant.

122. OCU materially breached the contract(s) it had entered with Plaintiff and Members of the Class by failing to safeguard such Personal Information and failing to notify them promptly of the intrusion into its computer systems that compromised such information. Defendant further breached the implied contracts with Plaintiff and Members of the Class by:

a. Failing to properly safeguard and protect Plaintiff' and Members of the Class's Personal Information;

b. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement; and

c. Failing to ensure the confidentiality and integrity of electronic Personal Information that Defendant received, maintained, and transmitted in violation of 45 C.F.R. § 164.306(a)(1).

123. The damages sustained by Plaintiff and Members of the Class as set forth in the preceding paragraphs were the direct and proximate result of Defendant's material breaches of its agreement(s).

124. Plaintiff and Members of the Class have performed as required under the relevant agreements, or such performance was waived by the conduct of Defendant.

125. The covenant of good faith and fair dealing is implied into every contract. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

126. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

127. Defendant failed to advise Plaintiff and Members of the Class of the Data Breach promptly and sufficiently.

128. In these and other ways, Defendant violated its duty of good faith and fair dealing.

129. Plaintiff and Members of the Class have sustained damages as a result of Defendant's breaches of its agreement, including breaches thereof through violations of the covenant of good faith and fair dealing.

COUNT IV
UNJUST ENRICHMENT

130. Plaintiff and Members of the Class incorporate the above allegations as if fully set forth herein.

131. This claim is pleaded in the alternative to the breach of express/implied contractual duty claim.

132. Plaintiff and Members of the Class conferred a benefit upon Defendant in the form of tuition fees in exchange for educational services or labor rendered in exchange for renumeration.

133. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiff and Members of the Class. Defendant also benefited from the receipt of Plaintiff's and Members of the Class's Personal Information, as this was required to facilitate the student and employment relationship, as well as for the purpose of applying for enrollment or employment.

134. As a result of Defendant's conduct, Plaintiff and Members of the Class suffered actual damages in an amount equal to the difference in value between the value of their tuition payments or labor with reasonable data privacy and security practices and procedures that Plaintiff and Members of the Class were entitled to, and that tuition or labor without reasonable data privacy and security practices and procedures that they received.

135. Under principals of equity and good conscience, Defendant should not be permitted to retain the monetary value of the tuition or labor belonging to Plaintiff and Members of the Class because Defendant failed to implement (or adequately implement) the data privacy and security practices and procedures for itself for which Plaintiff and Members of the Class expended tuition or labor and that were otherwise mandated by federal, state, and local laws and industry standards.

136. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Members of the Class all unlawful or inequitable proceeds received by it as a result of the conduct and Data Breach alleged herein.

COUNT V
INVASION OF PRIVACY

137. Plaintiff and Members of the Class incorporate the above allegations as if fully set

forth herein.

138. Defendant publicized private details and facts not generally known to the public, not publicly available, and not of legitimate public concern about Plaintiff and the Class Members by disclosing and exposing Plaintiff's and the Class Members' Personal Information to enough people that it is reasonably likely those facts have and/or will become known to the public at large, including, without limitation, on the dark web and elsewhere.

139. The disclosure of students' and employees' and prospective employees' full names, Social Security numbers, and financial information, is particularly harmful and would be offensive to a reasonable person of ordinary sensibilities.

140. Defendant has a special relationship with Plaintiff and the Class Members and Defendant's disclosure of Personal Information is certain to embarrass them and offend their dignity. Defendant should appreciate that the cyber-criminals who stole the Personal Information would fraudulently misuse that Personal Information, and further sell and disclose the data, just as they are doing. That the original disclosure is devastating to the Plaintiff and the Class Members, even though it originally may have only been disclosed to one person or a limited number of cyber-criminals, does not render it any less a disclosure to the public-at-large considering that said non-public information is now made public, and cannot be secured again.

141. The tort of public disclosure of private facts is recognized in Oklahoma. Plaintiff's and the Class Members' Personal Information was publicly disclosed by Defendant in the Data Breach with reckless disregard for the reasonable offensiveness of the disclosure. Such disclosure is highly offensive and would be to any person of ordinary sensibilities. Defendant knew or should have known that Plaintiff's and the Class Members' PII is not a matter of legitimate public concern.

142. As a direct and proximate result of Defendant's conduct, Plaintiff and Class

Members have been injured and are entitled to damages, as set forth herein.

COUNT VI
Violation of the Oklahoma Consumer Protection Act (15 O.S. § 751 *et seq.*)

143. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

144. In failing to promptly, fully and adequately disclose details surrounding the Data Breach, Defendant has violated the Oklahoma Consumer Protection Act ("OCPA").

145. Further, in its characterizations of the Data Breach, Defendant OCU utilized deceptive practices by – and through – its Notice Letter to Plaintiff and members of the Class.

146. Defendant OCU utilized unfair trade practices in representing the nature of the Data Breach as well as its purported efforts to rectify the Data Breach.

147. As detailed herein, Defendant OCU made false or misleading representations to Plaintiff and members of the Class as to the nature, characteristics, uses, and benefits of Defendant's purported efforts to rectify the Data Breach.

148. Since the OCPA parallels the FTC Act, Defendant's violations of the FTC Act explained, *supra*, constitute a violation of the OCPA too; especially those violations of the FTC Act concerning data security.

149. Defendant utilized these and other deceptive and unfair practices to work an unfair advantage over Plaintiff and members of the Class.

150. Plaintiff and member of the Class have incurred damages as a result of Defendant's violations of the OCPA.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, MARIA RUSKIEWICZ, individually and on behalf of all others similarly situated, the Class as heretofore identified, respectfully prays this Honorable Court for

judgment as follows:

A. Certification for this matter to proceed as a class action on behalf of the proposed Class under Fed. R. Civ. Proc. 23;

B. Designation of Plaintiff as Class Representative and designation of the undersigned as Class Counsel;

C. Actual damages in an amount according to proof;

D. Injunctive or declaratory relief;

E. Pre- and post-judgment interest at the maximum rate permitted by applicable law;

F. Costs and disbursements assessed by Plaintiff in connection with this action, including reasonable attorneys' fees pursuant to applicable law;

G. For attorneys' fees under the common fund doctrine and all other applicable law; and

H. Such other relief as this Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of herself and the Class, hereby demands a trial by jury pursuant to Fed. R. Civ. Proc. 38(b) on all claims so triable.

Dated: April 10, 2023

Respectfully submitted,

/s/ Matthew D. Alison
Jason B. Aamodt, OBA # 16974
Matthew D. Alison, OBA # 32723
INDIAN & ENVIRONMENTAL LAW GROUP, PLLC
406 South Boulder Ave., Suite 830
Tulsa, Oklahoma 74103
(918) 347-6169
(918) 948-6190 (facsimile)

jason@iaelaw.com
matthew@iaelaw.com

Lynn A. Toops*
Amina A. Thomas*
COHEN & MALAD LLP
One Indiana Square, Suite 1400
Indianapolis, Indiana 46204
(317) 636-6481
ltoops@cohenmalad.com
athomas@cohenmalad.com

J. Gerard Stranch, IV*
Andrew E. Mize*
STRANCH, JENNINGS & GARVEY, PLLC
223 Rosa L. Parks Avenue, Suite 200
Nashville, Tennessee 37203
(615) 254-8801
gstranch@stranchlaw.com gerards@bsjfirm.com
amize@stranchlaw.com andrewm@bsjfirm.com

Samuel Strauss*
Raina Borelli*
TURKE & STRAUSS, LLP
613 Williamson Street Suite 201
Madison, WI 53703
Ph: (608) 237-1775
Email: Sam@turkestrauss.com
Email: raina@turkestrauss.com

*Motion for *Pro Hac Vice* Admission to be made pursuant to Fed. R. Civ. Proc. 89(b)

Counsel for Plaintiff and the Proposed Class